



NEWSLETTER 6.2

'OUR NAME IS YOUR PROTECTION'

Name Your Favourite Grape – how we say thank you for referrals

If you have any business friends or associates who may need insurance advice or a new insurance broker, please let me know. I am happy to spend an hour or two with them – without cost – and if they become a client, I will send you a bottle of good quality New Zealand wine. You just need to name your favourite grape variety.

Risk Management

The number of claims that we are now handling compared to 3 years ago has risen substantially both in terms of numbers and dollar value. We draw your attention to **Page 2** on which we have detailed some excellent **staff fraud risk management tips** supplied by AIG Insurance.



John Barley

In response to certain patterns which we have noticed, we have set out below some tips of which we can probably all benefit from being reminded. The more we can minimise the risk, the less likely we are to be adversely affected – and with an improved claims record our premiums will positively reflect this. In this day and age of rising **petty theft** we again remind you of some simple risk management procedures which can significantly protect you from loss and inconvenience.

- **Never leave 'desirable' goods in your car - always put them in the boot.** Also be aware that whilst transferring goods from the car to your boot in a public place you are likely to be observed and can potentially give an impression of owning something worth stealing. The most desirable goods are cell phones, I-pods, wallets, laptops ...and **anything that looks like them**. Comment has been made "but it was only a laptop case, there was nothing in it" or "but my wallet was empty". The thief doesn't know that and can only find out by breaking your car window, resulting in inconvenience to you in getting it repaired. **If you leave items of this nature in your vehicle it is not a matter of 'if' it will be stolen, but 'when'.**
- **When absenting your vehicle for even short periods of time, always lock the vehicle.** There has been a spate of thefts from service stations made easy by drivers leaving their keys in the car. If you leave the keys in your car and it is stolen, it is highly unlikely that your insurer will honour the claim. Remember, that a condition of all insurance policies is that you must treat your assets as though you are uninsured.
- **Laptops** are a highly pilferable item and there have been a number of cases where thieves, **attired as repair people** or others who might legitimately be in the office (ie in a courier outfit with helmet, or in a white coat) enter premises and quickly uplift laptops from easily accessed areas. Please be aware of this risk because in larger offices where staff aren't personally aware of who provides repair services it has been known for staff to actually watch a thief calmly walk out of the office with stolen goods. If your office situation makes this a possibility it may be worth investing in a more secure reception area with entry buzzer.

With so many electronic items containing important information such as phone numbers, diaries and professional documentation **backup** of these items is of critical importance. Whether a loss of information is experienced because of hard drive crash on the PC, theft of your palm pilot or laptop, or simply dropping your high tech cell phone in a puddle – it can cause significant inconvenience and loss of irreplaceable essential information.

We recently experienced a hard drive crash which, as we had backed up only 4 hours earlier, did not result in any critical losses. However, even half a day of work by several staff can be substantial and with scrambled accounting records it did cause some inconvenience. If we had not backed up for several days that inconvenience would have been magnified. **Daily backups prevent significant loss of data.** Also remember to **keep backup disks away from the magnetic charge given out by TVs and microwaves** as it can scramble the data. **Backups should always be kept at a different site to the actual computer.** In this way, should there be a fire or theft, the backup will not be affected.

Continued on Page 2

'OUR NAME IS YOUR PROTECTION'

In ancient Celtic times Barley was used for protection and for prosperity.

An issue which has always been a concern and which appears to be escalating is **theft by staff**. No business is immune and losses can range from minor (although also expensive) theft of stamps, stationery, toll calls – through to significant financial theft. Recoveries after fraud tend to be low and over 60% of victims of crime said they had recovered less than 20% of their losses and with losses by managers and executives being 16 times greater than those caused by non-managerial staff. Just a simple random selection of recent claims equates to over \$2.1 million for only 9 claims (ranging in value from \$7,500 to \$1,035,000).

The best defence for your company is to identify and eliminate opportunities for staff theft to occur. Extracted from the AIG 'Fraud & Occupational Crime – A Serious Corporate Threat' Report are some simple methods of prevention:

- **Implement segregation of duties** (ie dual control procedures) so that no one person is permitted to control a transaction from beginning to end.
- **Ensure that reconciliation of bank statements is conducted regularly** and by persons other than those responsible for effecting banking transactions. Surprise checks and internal audits of those departments responsible for the management of the company's assets should be performed on a period basis.
- **Create a Code of Conduct** that covers such areas as conflicts of interest, third-party gifts and disclosure of confidential information, and requires all members of staff irrespective of seniority to sign and abide by such Code of Conduct. On a similar note, **draft and implement a Procedures Manual** that describes the duties of each grade of employee and the accompanying requirements to comply with such procedures. Ensure that prevention of insider fraud is a topic for regular discussion and review by senior management.
- **Appoint a senior official** to be responsible for insider **fraud prevention**. This individual should have experience in the field of fraud prevention or receive fraud prevention training. Membership of anti-fraud organisations, such as the Association of Certified Fraud Examiners, should also be encouraged, as well as regular co-operation and liaison with officials in other companies in the same lines of business. **Ensure that the Head of Internal Audit reports directly to the Board** to avoid filtering of information that could potentially conceal a fraud.
- **Implement a programme of fraud-awareness training** in order to highlight common trends in fraud and to inform staff of losses that other companies have suffered. The dissemination of information describing the potential cost of fraud to the company, how it manifests itself and how such fraud can be prevented and detected is instrumental in promoting a corporate 'anti fraud culture'. If implemented successfully fewer people will be tempted to commit fraud if only because they will be aware that their colleagues are alert to the dangers that insider crimes present to the company and possibly to their own livelihoods.
- **Install a free-to-call fraud 'hotline'** for all employees to use on an anonymous and confidential basis to report suspicious activity they observe or to voice concerns they wish to raise.
- In critical areas **implement a practice of short term job rotation and ensure that employees take vacations of at least one full week** (preferably two consecutive weeks) once a year during which time their duties are carried out by someone else.
- **Install software systems that require users to change their passwords at regular intervals.** Allowing employees access to another employee's password should be a disciplinary offence, as should the actual use of other persons' passwords. Implement procedures to ensure that passwords are withdrawn automatically when an employee's service is terminated or when password access is no longer required for an individual.
- In addition, fraud procedures should **specify a process for vetting vendors and suppliers** to include the invitation of prospective suppliers to tender in order to promote competition and avoid improper relationships with third parties. All payments to vendors and suppliers should be supported by original invoices that are marked 'paid' at the time of payment.
- Companies should avoid **placing too much trust in individuals** during times of administrative upheavals, such as those that occur in the **start up phase and both during and after mergers and acquisitions**. Extra vigilance is required for those businesses as they are especially susceptible to fraud during these times.

New Products

- In response to demand from the Avocado growing industry we have developed **tree insurance for avocado orchardists** in conjunction with a New Zealand insurer specialising in this market. The product covers damage to avocado trees caused by **fire, hail, earthquake, windstorm, volcanic eruption, malicious act and impact damage**. This product is also being rolled out to the **wine industry** which experiences similar issues with their vines and a crop cover is to follow.
- Although this product was launched late last year, for those involved in the residential investment market we draw your attention to the availability of cover for **Malicious Damage caused by Tenants**. If you are interested in this insurance extension please call us to discuss.

If you have any questions or wish to discuss any aspect of this newsletter please contact us.